



Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at <http://about.jstor.org/participate-jstor/individuals/early-journal-content>.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

*Invariantive Reduction of Quadratic Forms in the $GF[2^n]$.**

BY LEONARD EUGENE DICKSON.

1. In the **AMERICAN JOURNAL OF MATHEMATICS**, Vol. XXI (1899), I gave a complete set of non-equivalent canonical forms of m -ary quadratic forms in the Galois field of order p^n . The cases $p = 2$ and $p > 2$ are essentially different. In the opening pages of the present paper, I give a simpler treatment of the important case $p = 2$, a treatment bringing to the front some of the invariants of the form. In §§ 4, 5, I show that the rank r of the discriminantal determinant gives the minimum number of variables on which the form can be expressed. The definition of r in this modular theory differs from that in the algebraic theory in the employment of the halves of the minors of odd order. In particular, for m odd, the discriminant vanishes identically in the $GF[2^n]$, while the semi-discriminant S_m is an important invariant.

The larger part of the paper is devoted to the determination and application of a complete set of linearly independent invariants of the ternary † quadratic form $a_1 x_2 x_3 + \dots + \sum b_i x_i^2$ in the $GF[2^n]$ for $n \leq 4$. All the invariants may be expressed in terms of three fundamental independent invariants:

$$S_3 = a_1 a_2 a_3 + \sum a_i^2 b_i, \quad A = \prod_{i=1,2,3} (a_i^{2^{n-1}} - 1), \quad F = f + f^2 + f^4 + \dots + f^{2^{n-1}},$$

where f is a function increasing rapidly in complexity as n increases.

2. We consider the general m -ary quadratic form in the $GF[2^n]$:

$$Q_m(x) \equiv \sum_{i < j} c_{ij} x_i x_j + \sum b_i x_i^2 \quad (i, j = 1, \dots, m). \quad (1)$$

* Presented before the American Mathematical Society (Chicago), Dec. 30, 1906.

† For the invariants of binary quadratic forms in the $GF[p^n]$, for both $p > 2$ and $p = 2$, see *Transactions American Math. Soc.*, Vol. VIII (1907), pp. 205-232.

For the invariants of m -ary quadratic forms in the $GF[2]$, *i. e.*, with $n = 1$, see *Proceedings London Math. Soc.*, Ser. 2, Vol. V (1907), pp. 301-324.

If every $c_{ij} = 0$, we obtain the canonical form x_1^2 , since every mark is a square and $\sum b_i x_i^2 = [\sum b_i^2 x_i]^2$. In the contrary case, we may set $c_{12} \neq 0$. Then for

$$x'_1 = x_1 + \sum_{i=3}^m c_{2i} x_i, \quad x'_2 = c_{12}^{-1} x_2 + \sum_{i=3}^m c_{1i} x_i, \quad x'_j = c_{12} x_j (j > 2),$$

$Q_m(x')$ reduces* to

$$x_1 x_2 + c_{12} \sum_{i < j}^{3, \dots, m} [12ij] x_i x_j + b_1 x_1^2 + c_{12}^{-2} b_2 x_2^2 + \sum_{i=3}^m \beta_i x_i^2, \quad (2)$$

where $[12ij]$ denotes the Pfaffian $c_{12} c_{ij} - c_{1i} c_{2j} + c_{1j} c_{2i}$, and

$$\beta_i = c_{12} c_{1i} c_{2i} + b_1 c_{2i}^2 + b_2 c_{1i}^2 + b_i c_{12}^2. \quad (3)$$

For $m=3$, the vanishing of β_3 is a sufficient condition that (2) shall reduce to a binary form. It is also a necessary condition since, as shown below, β_3 is an invariant of Q_3 . Similarly, for $m=4$, the vanishing of the invariant $[1234]$ is the necessary and sufficient condition that (2), and hence Q_4 , shall be reducible to a ternary form.

Let next $m=5$. If every $[12ij] = 0$, (2) is reducible to a ternary form. In the contrary case, we may set $[1234] \neq 0$ and remove the terms $x_3 x_i, x_4 x_i$ ($i > 4$) by a transformation which adds to x_3 and x_4 suitable linear functions of x_5, \dots, x_m . Proceeding similarly, we conclude that either Q_m is expressible on fewer than m variables or else is reducible to

$$x_1 x_2 + x_3 x_4 + \dots + x_{m-2} x_{m-1} + x_m^2 \quad (m \text{ odd}), \quad (4)$$

$$x_1 x_2 + x_3 x_4 + \dots + x_{m-1} x_m + \sum_{i=1}^m \delta_i x_i^2 \quad (m \text{ even}). \quad (5)$$

The simple problem of the ultimate canonical forms of (5) is treated in § 6.

3. Although we shall derive independently (§ 4) the condition that Q_m shall reduce to a form in fewer than m variables, it seems worth while, in view of the peculiar character of the condition for m odd, to apply the preceding elementary method in the further examples $m=5$ and $m=6$.

When $m=5$, (2) is the sum of a binary form in x_1, x_2 , and a ternary form in x_3, x_4, x_5 . For the latter the ternary invariant (3) is c_{12}^2 times

$$c_{12} [1234] [1235] [1245] + \beta_3 [1245]^2 + \beta_4 [1235]^2 + \beta_5 [1234]^2.$$

On inserting the values (3) of the β_i , we find that the coefficients of b_1 and b_2 equal $c_{12}^2 [2345]^2$ and $c_{12}^2 [1345]^2$, respectively, in view of the algebraic identity

$$c_{23} [1245] - c_{24} [1235] + c_{25} [1234] \equiv c_{12} [2345].$$

* It is simpler to verify that, under the inverse transformation, (2) becomes $Q(x')$.

Further, the part independent of the b 's is seen to equal $c_{12}^2 \psi$, where

$$\psi = \sum_{(12)} c_{12} c_{13} c_{24} c_{35} c_{45} - \sum_{(10)} c_{12}^2 c_{34} c_{35} c_{45}, \quad (6)$$

where the first sum extends over the 12 products in which each subscript occurs exactly twice. Dropping the factor c_{12}^2 , we obtain the invariant

$$\phi = \psi + b_1 [2345]^2 + b_2 [1345]^2 + \dots + b_5 [1234]^2, \quad (7)$$

whose vanishing is the condition that Q_5 be reducible to a quaternary form.

For $m = 6$, the quaternary invariant for the terms x_3, \dots, x_6 of (2) is

$$[1234] [1256] - [1235] [1246] + [1236] [1245],$$

which is (algebraically) c_{12} times the Pfaffian $[123456]$.

4. The algebraic discriminant of the form (1) is

$$\Delta = \begin{vmatrix} 2b_1 & c_{12} & c_{13} & \dots & c_{1m} \\ c_{12} & 2b_2 & c_{23} & \dots & c_{2m} \\ \dots & \dots & \dots & \dots & \dots \\ c_{1m} & c_{2m} & c_{3m} & \dots & 2b_m \end{vmatrix}.$$

In the $GF[2^n]$, this determinant is skew symmetric, and hence vanishes for m odd, while for m even it equals the square of the Pfaffian $[12 \dots m]$.

For m odd, we define the *semi-discriminant* S_m of the form Q_m in the $GF[2^n]$ to be the expression derived *algebraically* by dividing by 2 each of the (even) coefficients in the expansion of Δ . Thus S_3 is β_3 and S_5 is ϕ , given by (3) and (7), respectively; indeed, Δ is congruent modulo 4 to $2\beta_3$ and 2ϕ , respectively.

Note that in Q_m any coefficient may be increased by a multiple of 2; but Δ is thereby increased by a multiple of 4, so that S_m is unaltered modulo 2.

All m -ary linear homogeneous transformations with coefficients in any given field F can be derived from generators of the two types:

$$x_1 = x'_1 + t x'_2, \quad x_i = x'_i \quad (i > 1); \quad (8)$$

$$x_1 = \lambda x'_1, \quad x_i = x'_i \quad (i > 1). \quad (9)$$

Under these transformations Q becomes Q' , with the (altered) coefficients:

$$b'_2 = b_2 + t c_{12} + t^2 b_1, \quad c'_{12} = c_{12} + 2t b_1, \quad c'_{2i} = c_{2i} + t c_{1i} \quad (i = 3, \dots, m); \quad (8')$$

$$b'_1 = \lambda^2 b_1, \quad c'_{1i} = \lambda c_{1i} \quad (i = 2, \dots, m). \quad (9')$$

For (9'), $\Delta' = \lambda^2 \Delta$, since we may remove the factor λ from the first row and column. For (8'), Δ' becomes Δ if we subtract t times the elements of the first row from the second, and then subtract t times the elements of the first column

from the second. From this formal algebraic result we conclude, in view of the remark in the preceding paragraph, that S_m is a relative invariant in the $GF[2^n]$. But $S_m \equiv 1$ for (4), $\Delta \equiv 1$ for (5), while $S_m \equiv 0$ and $\Delta \equiv 0$ for forms in fewer than m variables. Hence follows the

THEOREM: *According as m is even or odd, the vanishing of the (invariant) discriminant or semi-discriminant is the necessary and sufficient condition that an m -ary quadratic form in the $GF[2^n]$ shall be linearly transformable into a form of fewer than m variables.*

5. Suppose that, for m odd, S_m vanishes in the $GF[2^n]$, while not all the first minors M_{ij} of Δ vanish. Under a suitable linear transformation, Q_m becomes Q'_m , lacking the variable x_m . In the discriminant of Q'_m , the minor M'_{mm} alone does not vanish, since the M_{ij} are linear functions of it. Hence Q_m is expressible on $m-1$, but not on fewer, variables (§ 4).

Suppose that, for m even, the discriminant Δ vanishes in the $GF[2^n]$. Then all its first minors M_{ij} vanish. Indeed, $M_{ii} M_{jj} - M_{ij} M_{ji}$ is the product of Δ and a minor of degree $m-2$. But $M_{ii} \equiv M_{jj} \equiv 0 \pmod{2}$, and $M_{ij} = M_{ji}$. Hence the M_{ij} may be assumed* to have the factor 2 algebraically, so that the *semi-minors* are unambiguously defined in the $GF[2^n]$. If the latter do not all vanish, Q_m is expressible on $m-1$, but not on fewer, variables (§ 4).

Combining our results, we obtain the

THEOREM: *In order that a quadratic form Q_m in the $GF[2^n]$ shall be reducible under linear transformation in the field to a quadratic form on r variables, but not reducible to one on less than r variables, it is necessary and sufficient that in the discriminantal determinant of Q_m every $\mu^{(m)}, \dots, \mu^{(r+1)}$ shall vanish, but not every $\mu^{(r)}$, where $\mu^{(s)}$ ranges over the minors or semi-minors of order s , according as s is even or odd.*

6. It remains to complete the reduction of F_m , given by (5). We first reduce it to the form

$$x_1 x_2 + x_3 x_4 + \dots + x_{m-1} x_m + x_1^2 + \delta x_2^2, \quad \delta \equiv \delta_1 \delta_2 + \dots + \delta_{m-1} \delta_m. \quad (5')$$

If every $\delta_i = 0$, no reduction is necessary. In the contrary case we may set $\delta_1 \neq 0$. Applying to $F_4(x'')$ in succession the three transformations:

$$x_1''' = \delta_1^{-\frac{1}{2}} x_1'', \quad x_2''' = \delta_1^{\frac{1}{2}} x_2''; \quad x_1'' = x_1' + \delta_3^{\frac{1}{2}} x_3', \quad x_4'' = x_4' + \delta_3^{\frac{1}{2}} x_2'; \quad x_3' = x_3 + \delta_4 x_4,$$

we obtain $x_1 x_2 + x_3 x_4 + x_1^2 + (\delta_1 \delta_2 + \delta_3 \delta_4) x_2^2$. Hence from F_m we reach (5').

* In case $n > 1$, we first eliminate the n^{th} and higher powers of the root of the irreducible congruence $(\text{mod } 2)$ defining the $GF[2^n]$.

Now* $x_1 x_2 + x_1^2 + \delta x_2^2$ is reducible in the $GF[2^n]$ if $\chi(\delta) = 0$, but is irreducible if $\chi(\delta) = 1$, where

$$\chi(\delta) \equiv \delta + \delta^2 + \delta^4 + \dots + \delta^{2^{n-1}}. \quad (10)$$

The 2^{n-1} forms (5') with $\chi(\delta) = 1$ are all equivalent,* but not reducible to one of the 2^{n-1} forms with $\chi(\delta) = 0$. The latter are evidently reducible to

$$x_1 x_2 + x_3 x_4 + \dots + x_{m-1} x_m. \quad (11)$$

The forms (5) constitute two non-equivalent classes characterized by the vanishing on non-vanishing of $\chi(\delta)$, $\delta \equiv \delta_1 \delta_2 + \dots + \delta_{m-1} \delta_m$.

It may be shown that $\chi(\delta)$ is an absolute invariant of the group of all linear transformations in the $GF[2^n]$ which preserve the *system* of forms (5).

7. We next seek a condition on the coefficients of the quadratic form Q_m (m even), of non-vanishing discriminant Δ in the $GF[2^n]$, which shall characterize à priori the class (§ 6) to which Q_m belongs. If $n = 1$, we have $\Delta = 1$ in the field. For any n , we shall assume, for the present, that $\Delta = 1$ (a slight normalization accomplished, for instance, by multiplying one of the variables by the mark $\Delta^{-\frac{1}{2}}$). In view of § 6, we may state our desiderata as follows: We seek a function ϕ of the coefficients of the form Q_m (m even) of discriminant unity, such that ϕ becomes $\chi(\delta)$ when Q_m specializes to (5), and such that ϕ is an absolute invariant of Q_m under the group of all m -ary linear homogeneous transformations of determinant unity in the $GF[2^n]$.

For $m = 2$, the problem is solved, since $\Delta = 1$ implies $c_{12} = 1$, whence

$$Q_2 = x_1 x_2 + b_1 x_1^2 + b_2 x_2^2, \quad \phi = \chi(b_1 b_2).$$

For $m = 4$, we apply to (5) the transformation (of determinant unity),

$$x_1 = \xi_1 + c_{23} \xi_3 + c_{24} \xi_4, \quad x_2 = \xi_2 + c_{13} \xi_3 + c_{14} \xi_4, \quad x_3 = \xi_3, \quad x_4 = \xi_4,$$

and obtain a form $Q_4(\xi)$ in which

$$\begin{aligned} c_{12} &= 1, \quad c_{34} = 1 + c_{13} c_{24} + c_{14} c_{23}, \quad b_1 = \delta_1, \quad b_2 = \delta_2, \\ b_3 &= \delta_3 + c_{13} c_{23} + \delta_1 c_{23}^2 + \delta_2 c_{13}^2, \quad b_4 = \delta_4 + c_{14} c_{24} + \delta_1 c_{24}^2 + \delta_2 c_{14}^2. \end{aligned}$$

Hence by choice of the δ 's the resulting form may be made identical with any form Q_4 in which $c_{12} = 1$, $[1234] = 1$. The last condition is equivalent to our assumption $\Delta = 1$ on Q_4 . The restriction, $c_{12} = 1$, on the generality of Q_4 will be overcome by symmetry, as demanded by the invariance of ϕ . Expressing

* AMERICAN JOURNAL, l. c., p. 224; *Linear Groups*, p. 199.

$\delta_1 \delta_2 + \delta_3 \delta_4$ in terms of the c_{ij} , b_i , and applying $c_{12} = 1$, $[1234] = 1$, we get $\psi + \rho + \rho^2$, where $\rho = b_1 c_{23} c_{24} + b_2 c_{13} c_{14} + c_{12} c_{34}$, and

$$\psi = \sum_{(6)} b_1 b_2 c_{34}^2 + \sum_{(4)} b_1 c_{23} c_{24} c_{34} + \sum_{(8)} c_{13} c_{14} c_{23} c_{24}. \quad (12)$$

Then $\chi(\delta_1 \delta_2 + \delta_3 \delta_4)$ becomes $\chi(\psi)$ since $\chi(\rho + \rho^2) = 0$ in the field. Now $\phi \equiv \chi(\psi)$ has the required properties. It remains only to show that ϕ is an absolute invariant of Q_4 under the group of all quaternary linear transformations of determinant unity. In view of the symmetry of (12), we may restrict the proof to the generator (8). Here (8') becomes

$$b'_2 = b_2 + tc_{12} + t^2 b_1, \quad c'_{23} = c_{23} + tc_{13}, \quad c'_{24} = c_{24} + tc_{14}.$$

Under this transformation, the increment to ψ is

$$tb_1 c_{34} [1234] + t^2 b_1^2 c_{34}^2 + tc_{13} c_{14} [1234] + t^2 c_{13}^2 c_{14}^2,$$

and hence is of the form $\sigma + \sigma^2$, since $[1234] = 1$. Hence the increment to $\phi = \chi(\psi)$ is $\chi(\sigma + \sigma^2) = 0$, so that ϕ is an absolute invariant.

8. We next consider the determination of functions of the coefficients of Q_m which are invariant under every m -ary linear homogeneous transformation in the $GF[2^n]$.

As the independent invariants of Q_2 we may take *

$$c_{12}, \quad (c_{12}^{2^n-1} - 1) (b_1^{2^n-1} - 1) (b_2^{2^n-1} - 1), \quad \chi(b_1 b_2 c_{12}^{2^n-3}),$$

where χ is defined by (10). For $n = 1$, we take $\chi(b_1 b_2 c_{12})$.

In the remainder of this paper we shall discuss Q_3 for low values of n .

9. Consider the ternary quadratic form in the $GF[2^n]$,

$$a_1 x_2 x_3 + a_2 x_1 x_3 + a_3 x_1 x_2 + \sum b_i x_i^2. \quad (13)$$

We tabulate, for reference, a set of generators of the ternary linear group, and give the (altered) coefficients of the transformed quadratic form:

$$x_1 = x'_1 + tx'_2: \quad a'_1 = a_1 + ta_2, \quad b'_2 = b_2 + t^2 b_1 + ta_3; \quad (14)$$

$$x_1 = \lambda x'_1: \quad a'_2 = \lambda a_2, \quad a'_3 = \lambda a_3, \quad b'_1 = \lambda^2 b_1; \quad (15)$$

$$(x_i x_j): \quad (a_i a_j) (b_i b_j). \quad (16)$$

We readily verify * the absolute invariance of

$$A = \prod (a_i^{2^n-1} - 1), \quad I = A \prod (b_i^{2^n-1} - 1) \quad (i = 1, 2, 3). \quad (17)$$

* *Transactions Amer. Math. Soc.*, Vol. VIII (1907), pp. 514-522.

10. Let first $n = 1$, so that we consider the invariants of the ternary cubic (13) modulo 2. Let ϕ be a polynomial in the a 's and b 's with exponents 0 or 1. We may set

$$\phi = p + qa_1 + jb_2 + ka_1 b_2 \quad (p, q, j, k \text{ independent of } a_1, b_2).$$

Now ϕ is invariant under (14), with $t = 1$, if and only if

$$a_2 \frac{\partial \phi}{\partial a_1} + (b_1 + a_3) \frac{\partial \phi}{\partial b_2} + a_2 (b_1 + a_3) \frac{\partial^2 \phi}{\partial a_1 \partial b_2} \equiv 0 \pmod{2}.$$

The conditions are:

$$a_2 k \equiv 0, \quad (b_1 + a_3) k \equiv 0, \quad a_2 q + (b_1 + a_3) j \equiv 0. \quad (18)$$

From the first two,

$$k = (a_2 + 1) \{l(1 + b_1 + a_3) + mb_1 a_3\},$$

where l and m are (linear) functions of b_3 only. By subtracting from ϕ a suitable multiple of the invariant I , we may assume that m is independent of b_3 . Hence no term of ϕ has the factor $a_1 b_2 \cdot b_1 a_3 \cdot b_3$. Applying the permutation [23], we see that no term of ϕ has the factor $a_1 b_2 a_2 b_1 b_3$. Hence l is independent of b_3 . Applying the permutation [13] we obtain the terms with the factor $a_3 b_2$:

$$a_3 b_2 (a_2 + 1) \{l(1 + b_3 + a_1) + mb_3 a_1\}.$$

Hence those multiplying $a_1 b_2 a_3 (a_2 + 1)$ are $l + mb_3$. In the initial form of ϕ , the corresponding terms were $l + mb_1$. Hence $m \equiv 0$ and

$$k = l(a_2 + 1)(1 + b_1 + a_3), \quad l = 0 \text{ or } 1.$$

In view of the terms multiplying $a_3 b_2$, we have

$$j = la_3(a_2 + 1)(1 + b_3) + \alpha + \beta a_2 + \gamma b_1 + \delta a_2 b_1,$$

where $\alpha, \beta, \gamma, \delta$ are functions of b_3 only. By (18₃), $(b_1 + a_3)j$ must have the factor a_2 . Hence

$$\alpha \equiv \gamma \equiv l(b_3 + 1).$$

The terms of ϕ multiplying b_2 are $j + ka_1$. Hence those multiplying $b_1 b_2$ are $\gamma + \delta a_2 + la_1(a_2 + 1)$. Since these must be symmetrical in a_1, a_2 , we have $\delta \equiv l$. Set $\beta = \beta_1 + \beta_2 b_3$. Then the terms multiplying $b_2 b_3$ are:

$$la_3(a_2 + 1) + l + \beta_2 a_2 + lb_1.$$

These must be symmetrical in a_2, a_3 . Hence $\beta_2 \equiv l$, and

$$j = la_3(a_2 + 1)(b_3 + 1) + l(b_1 + 1)(b_3 + 1) + la_2(b_1 + b_3) + \beta_1 a_2.$$

The terms $j + ka_1$, which multiply b_2 , may now be written in the form

$$lb_1 b_3 + lb_1 (a_1 + 1) (a_2 + 1) + lb_3 (a_2 + 1) (a_3 + 1) + l(a_1 + 1) (a_2 + 1) (a_3 + 1) + (l + \beta_1) a_2.$$

Those multiplying b_1 or b_3 may be obtained by symmetry. Hence

$$\phi = lK + (l + \beta_1) \sum a_i b_i + \psi,$$

where ψ is a function of a_1, a_2, a_3 only, while

$$K = b_1 b_2 b_3 + \sum b_i b_j (a_i + 1) (a_j + 1) + (\sum b_i) A \quad (i, j = 1, 2, 3; i \neq j), \quad (19)$$

$A = \prod (a_i + 1)$ being the invariant (17) for $n = 1$. We may set

$$\psi = \lambda a_1 a_2 a_3 + \mu \sum a_i a_j + \nu \sum a_i.$$

Then the terms multiplying a_1 , but not b_2 , are:

$$q = l \{ b_1 b_3 (a_3 + 1) + (b_1 + b_3) (a_2 + 1) (a_3 + 1) + b_1 \} + \beta_1 b_1 + \lambda a_2 a_3 + \mu (a_2 + a_3) + \nu.$$

Then (18₃) gives $l + \beta_1 + \lambda + \mu \equiv 0, \mu \equiv \nu$. The invariant ϕ thus involves three arbitrary parameters l, λ, μ . Giving in turn one of these the value 1 and the other two the value 0, we obtain the invariants K and

$$S_3 = a_1 a_2 a_3 + \sum a_i b_i, \quad I_2 = \sum a_i b_i + \sum a_i a_j + \sum a_i,$$

S_3 occurring in § 4. Now $S_3 + I_2 + 1 = A$, while $K + A$ equals

$$J = \{b_1 + (a_2 + 1) (a_3 + 1)\} \{b_2 + (a_1 + 1) (a_3 + 1)\} \{b_3 + (a_1 + 1) (a_2 + 1)\}. \quad (20)$$

In the GF[2] the four linearly independent invariants of the ternary quadratic form (13) may be taken to be A, I, S_3, J .

11. Let next $n = 2$, so that we consider the invariants of the ternary cubic (13) in the $GF[2^2]$. Under transformation (14), let a polynomial ϕ , with exponents ≤ 3 , become ϕ' . We employ the abbreviations:

$$(1^i) = \frac{1}{i!} \frac{\partial^i \phi}{\partial a_1^i}, \quad (2^i) = \frac{1}{i!} \frac{\partial^i \phi}{\partial b_2^i}, \quad (1^i 2^j) = \frac{1}{i! j!} \frac{\partial^{i+j} \phi}{\partial a_1^i \partial b_2^j},$$

in which the division of the algebraic derivatives by $i!$ and $j!$ is to be performed algebraically and the quotients alone interpreted in the $GF[2^2]$. Then

$$\phi' - \phi = \tau_1 t + \tau_2 t^2 + \tau_3 t^3,$$

$$\begin{aligned} \tau_1 &= a_2 (1) + a_3 (2) + b_1^2 (2^2) + a_2^2 b_1 (1^2 2) + a_3^2 b_1 (2^3) + a_2^3 a_3 (1^3 2) \\ &\quad + a_2^2 a_3^2 (1^2 2^2) + (a_2 b_1^3 + a_2 a_3^3) (1 2^3) + a_2^3 b_1^2 (1^3 2^2) + a_2^2 a_3 b_1^2 (1^2 2^3) \\ &\quad + a_2^3 a_3^2 b_1 (1^3 2^3), \end{aligned}$$

$$\begin{aligned}\tau_2 &= b_1(2) + a_2^2(1^2) + a_2 a_3(1 2) + a_3^2(2^2) + a_2 b_1^2(1 2^2) + a_3 b_1^2(2^3) \\ &\quad + a_2^3 b_1(1^3 2) + a_2 a_3^2 b_1(1 2^3) + a_2^3 a_3^2(1^3 2^2) + (a_2^2 b_1^3 + a_2^2 a_3^3)(1^2 2^3) \\ &\quad + a_2^3 a_3 b_1^2(1^3 2^3), \\ \tau_3 &= a_2 b_1(1 2) + a_2^3(1^3) + a_2^2 a_3(1^2 2) + a_2 a_3^2(1 2^2) + (a_3^3 + b_1^3)(2^3) \\ &\quad + a_2^2 b_1^2(1^2 2^2) + a_2 a_3 b_1^2(1 2^3) + a_2^2 a_3^2 b_1(1^2 2^3) + (a_2^3 b_1^3 + a_2^3 a_3^3)(1^3 2^3).\end{aligned}$$

We may set

$$\phi = \sum_{i,j}^{0, 1, 2, 3} A_{ij} a_1^i b_2^j \quad (A_{ij} \text{ independent of } a_1, b_2).$$

When this expression is inserted, τ_1, τ_2, τ_3 must vanish* identically in a_1, b_2 . From the coefficients of $b_2^3 a_1^2, b_2^2 a_1^3, b_2 a_1^3, b_2^3, b_2^2 a_1, b_2 a_1$ in τ_1 , we get:

$$A_{33} a_2 = A_{33} a_3 = A_{33} b_1 = 0, \quad A_{13} a_2 = A_{13} a_3 = A_{13} b_1 = 0. \quad (21)$$

Hence must $A_{33} = \alpha\pi, A_{13} = \beta\pi$, where

$$\pi = (a_2^3 - 1)(a_3^3 - 1)(b_1^3 - 1),$$

while α and β are functions of b_3 only. Hence the factor of $a_1^3 a_3^3 b_2^3$ in ϕ is

$$\alpha(a_2^3 - 1)(b_1^3 - 1).$$

This must be symmetrical in b_1 and b_3 . Hence $\alpha = \alpha_0(b_3^3 - 1)$, where α_0 is a constant mark. Thus ϕ has the term

$$\alpha_0 a_1^3 a_2^3 a_3^3 b_1^3 b_2^3 b_3^3,$$

which is unaltered by (15). If ϕ is not an absolute invariant, $\alpha_0 = 0$. If ϕ is an absolute invariant, we replace ϕ by $\phi - \alpha_0 I$, where I is the absolute invariant (17)_{n=2}. In either case, it remains to consider an invariant ϕ having $\alpha_0 = 0$. Since $A_{33} = 0$, ϕ has no term with the factor $a_1^3 b_2^3$. Applying suitable permutations of the subscripts, we conclude that

$$A_{33} = A_{13} = 0; \text{ no term of } \phi \text{ has a factor } a_i^3 b_j^3 \text{ or } a_i b_i^3 \quad (i \neq j). \quad (22)$$

From the coefficients of $b_2^3, a_1^2 b_2, a_1^2 b_2^2, a_1 b_2, a_1 b_2^2$ in τ_2 with $A_{33} = A_{13} = 0$, we get:

$$A_{23} a_2 = A_{23} a_3 = A_{23} b_1 = 0, \quad A_{31} a_2 = A_{32} a_2 = 0. \quad (23)$$

By the first three and (22),

$$A_{23} = 0; \text{ no term of } \phi \text{ has a factor } a_i^2 b_j^3 \quad (i \neq j). \quad (24)$$

* Note that $\tau_1 = 0$ does not imply $\tau_2 = 0$ as in the algebraic theory. In fact, for

$$\phi = a_1^3 a_2^3 a_3^3 + a_1 b_1 a_2^2 a_3^2 + a_2 b_2 a_1^2 a_3^2 + a_3 b_3 a_1^2 a_2^2,$$

$$\tau_1 = 0, \text{ but } \tau_2 \neq 0.$$

With the simplifications $A_{13} = A_{23} = A_{33} = 0$, $A_{31}a_2 = A_{32}a_2 = 0$, we find as the conditions for $\tau_1 = 0$; $\tau_2 = 0$ (identically in a_1 , b_2):

$$A_{31}a_3 = A_{32}b_1^2, \quad A_{12}a_2 = A_{03}a_3, \quad A_{11}a_2 = A_{03}b_1^2, \quad (25)$$

$$A_{30}a_2 + A_{21}a_3 + A_{22}b_1^2 = 0, \quad A_{11}a_3 = A_{12}b_1^2, \quad (26)$$

$$A_{10}a_2 + A_{01}a_3 + A_{02}b_1^2 + A_{21}a_2^2b_1 + A_{03}a_3^2b_1 + A_{22}a_2^2a_3^2 = 0; \quad (27)$$

$$A_{32}a_3^2 = A_{31}b_1, \quad A_{22}a_3^2 = A_{21}b_1, \quad A_{03}a_3^2 = A_{21}a_2^2, \quad (28)$$

$$A_{22}a_2^2 = A_{03}b_1, \quad A_{30}a_2^2 + A_{12}a_3^2 + A_{11}b_1 = 0, \quad (29)$$

$$A_{20}a_2^2 + A_{02}a_3^2 + A_{12}a_2b_1^2 + A_{01}b_1 + A_{11}a_2a_3 + A_{03}a_3b_1^2 = 0. \quad (30)$$

Finally, τ_3 becomes

$$(A_{11}a_2 + A_{03}b_1^2)b_1 + (A_{12}a_2 + A_{03}a_3)a_3^2 + (A_{30}a_2 + A_{21}a_3 + A_{22}b_1^2)a_2^2,$$

and hence is zero by (22) and (26₁). We multiply (28₂) by a_2^2 and apply to (27); we multiply (26₂) by a_2 and apply to (30); there result:

$$A_{10}a_2 + A_{01}a_3 + A_{02}b_1^2 + A_{03}a_3^2b_1 = 0, \quad A_{20}a_2^2 + A_{02}a_3^2 + A_{01}b_1 + A_{03}a_3b_1^2 = 0. \quad (31)$$

A polynomial ϕ , lacking the highest term of I , will be an invariant if and only if it be unaltered by the simple transformations (15), (16), and satisfy conditions (22), (23₄), (23₅), (24), (25), (26), (28), (29) and (31).

Denote the general term of ϕ by

$$a_1^{e_1}a_2^{e_2}a_3^{e_3}b_1^{f_1}b_2^{f_2}b_3^{f_3}. \quad (32)$$

The conditions that ϕ shall be unaltered by the transformations of type (15) are:

$$e_2 + e_3 + 2f_1 \equiv e_1 + e_3 + 2f_2 \equiv e_1 + e_2 + 2f_3 \equiv d \pmod{3}, \quad (33)$$

where d is a fixed integer such that $\phi' = D^d\phi$ for a transformation of determinant D . We treat in turn the cases $d = 0$, $d = 1$, $d = 2$.

12. Let first ϕ be an absolute invariant, so that $d \equiv 0$, and

$$f_1 \equiv e_2 + e_3, \quad f_2 \equiv e_1 + e_3, \quad f_3 \equiv e_1 + e_2 \pmod{3}. \quad (33')$$

For the terms $A_{32}a_1^3b_2^2$, $e_1 = 3$, $f_2 = 2$, so that $e_3 = 2$. By (23₅), a_2 occurs in A_{32} only in the combination $a_2^3 - 1$. Hence $e_2 \equiv 0 \pmod{3}$, $f_1 = 2$, $f_3 = 0$ or 3. By (22), the factor $a_1^3b_3^3$ does not occur. Hence

$$A_{32} = r a_3^2 b_1^2 (a_2^3 - 1), \quad r = \text{constant}. \quad (34)$$

Proceeding similarly with A_{31} , and determining the constant by either (25₁) or (28₁), we get

$$A_{31} = r a_3 b_1 (a_2^3 - 1). \quad (35)$$

Listing the possible terms (32) of A_{03} , A_{12} , A_{11} , in view of (33'), (22), (31), and imposing conditions (25₂), (25₃), (26₂), we readily find that:

$$A_{03} = \lambda a_2^3 + \mu a_2 b_1 b_3 + \nu a_2^2 b_1^2 b_3^2, \quad (36)$$

$$A_{12} = \lambda a_2^2 a_3 + \mu a_3 b_1 b_3 + \nu a_2 a_3 b_1^2 b_3^2, \quad (37)$$

$$A_{11} = \lambda a_2^2 b_1^2 + \mu b_1^3 b_3 + \nu a_2 b_1 b_3^2 + l b_3 (a_2^3 - 1) (a_3^3 - 1). \quad (38)$$

Applying conditions (26₁), (28₂), (28₃), (29), and requiring that the factor $\sum A_{3i} b_2^i$ of a_1^3 in ϕ shall be unaltered by [23], we find that:

$$l = \mu = \nu = r, \quad (39)$$

$$A_{30} = r(a_2 b_1 b_3 + a_2^2 b_1^2 b_3^2)(a_3^3 - 1) + s(a_2^3 - 1)(a_3^3 - 1) + \lambda a_2^3 a_3^3 + \lambda b_1^3, \quad (40)$$

$$A_{21} = r a_3^2 b_1^2 b_3^2 + r a_2^2 a_3^2 b_1 b_3 + \lambda a_2 a_3^2, \quad (41)$$

$$A_{22} = r b_3^2 (a_2^3 - 1)(a_3^3 - 1) + r b_1^3 b_3^2 + r a_2^2 b_1^2 b_3 + \lambda a_2 b_1. \quad (42)$$

Since the factors $\sum A_{1i} b_2^i$ and $\sum A_{2i} b_2^i$ of a_1 and a_1^2 must be unaltered by [23], while the factors $\sum A_{i1} a_1^i$ and $\sum A_{i2} a_1^i$ of b_2 and b_2^2 must be unaltered by [13]:

$$A_{10} = \lambda a_3^2 b_1^2 b_3 + \lambda a_2 a_3^2 b_3^2 + q a_2^2 a_3^2 b_1, \quad (43)$$

$$A_{20} = \lambda a_3 b_1 b_3^2 + \lambda a_2^2 a_3 b_3 + p a_2 a_3 b_1^2, \quad (44)$$

$$A_{01} = r a_3 b_1 + r a_3 b_1 b_3^2 + r a_2 a_3 b_1^2 b_3 + r a_2^3 a_3 b_1 + \lambda a_2^2 a_3 b_3^2, \quad (45)$$

$$A_{02} = r a_3^2 b_1^2 + r a_3^2 b_1^2 b_3^2 + r a_2^2 a_3^2 b_1 b_3^2 + r a_2^3 a_3^2 b_1^2 + \lambda a_2 a_3^2 b_3. \quad (46)$$

Conditions (31) require merely that

$$q = p = \lambda. \quad (47)$$

Since the terms $\sum A_{0i} b_2^i$, independent of a_1 , must be unaltered by [23]; and the terms $\sum A_{i0} a_1^i$, independent of b_2 , must be unaltered by [13]:

$$A_{00} = r(a_2 b_1 b_3 + a_2^2 b_1^2 b_3^2)(a_3^3 - 1) + s(a_2^3 - 1)(a_3^3 - 1) + \lambda a_3^3 b_3^3, \quad (48)$$

in which the constant term of ϕ has been taken to be s .

The A_{ij} have been so determined that ϕ is unaltered by the generators (14)–(16) of the ternary linear group in the $GF[2^2]$. Hence the resulting function ϕ is an absolute invariant. Of the parameters occurring in the above expressions for the A_{ij} , r , s and λ may be given arbitrary values in the field, while the remaining parameters are then determined by (39) and (47).

For $s = 1$, $r = \lambda = 0$, ϕ is the invariant A in (17) for $n = 2$.

For $\lambda = 1$, $r = s = 0$, $\phi = S_3^3$, where (§ 4)

$$S_3 = a_1 a_2 a_3 + a_1^2 b_1 + a_2^2 b_2 + a_3^2 b_3. \quad (49)$$

Finally, for $r = 1$, $s = \lambda = 0$, ϕ is the absolute invariant

$$\left. \begin{aligned} F = f + f^2, \quad f \equiv & a_1 b_1^3 b_2 b_3 + a_2 b_2^3 b_1 b_3 + a_3 b_3^3 b_1 b_2 + a_1 a_2 a_3 b_1^2 b_2^2 b_3^2 \\ & + a_1 a_2 b_1 b_2 b_3^2 + a_1 b_2 b_3 (a_2^3 - 1)(a_3^3 - 1) \\ & + a_1 a_3 b_1 b_3 b_2^2 + a_2 b_1 b_3 (a_1^3 - 1)(a_3^3 - 1) \\ & + a_2 a_3 b_2 b_3 b_1^2 + a_3 b_1 b_2 (a_1^3 - 1)(a_2^3 - 1). \end{aligned} \right\} \quad (50)$$

The four linearly independent absolute invariants of the ternary quadratic form (13) in the $GF[2^2]$ may be taken to be A and I , given by (17), S_3^3 and F , given by (49) and (50).

We note the relation $S_3 F = 0$.

13. We next readily prove that the only relative invariants of (13) are S_3 and S_3^2 . It suffices to consider the case in which $d \equiv 2$ in (33). For, if $d \equiv 1$ and $\phi'_1 = D\phi_1$, then $\phi' = D^2\phi$, where $\phi = \phi_1^2$. Since we shall prove that $\phi = S_3$, it follows that $\phi_1 = (\phi_1^2)^2 = S_3^2$.

Let therefore $d \equiv 2$ (mod 3). Then, by (33),

$$f_1 \equiv e_2 + e_3 + 1, \quad f_2 \equiv e_1 + e_3 + 1, \quad f_3 \equiv e_1 + e_2 + 1. \quad (33'')$$

For the terms (32) of $A_{03}b_2^3$, $e_1 = 0$, $f_2 = 3$, so that $e_3 = 2$. But by (31), the factor $a_3^2 b_2^3$ cannot occur. Hence $A_{03} \equiv 0$. Then by (25₂), (25₃), (28₃), (29₁),

$$A_{12}a_2 = A_{11}a_2 = A_{21}a_2 = A_{22}a_2 = 0,$$

so that, in these A_{ij} , a_2 occurs only in the combination $a_2^3 - 1$, whence $e_2 \equiv 0$ (mod 3). Hence for A_{12} , $e_1 = 1$, $f_2 = 2$, $e_3 \equiv 0$ (mod 3), $f_1 = 1$, $f_3 = 2$. Hence A_{12} has the factor b_1 . For A_{11} , $e_3 = 2$, $f_3 = 2$, $f_1 = 0$, 3; but $a_3^2 b_1^3$ is not a factor. Hence b_1 occurs in no term of A_{11} . Hence, by (26₂), $A_{11} \equiv A_{12} \equiv 0$. Similarly, A_{21} has the factor b_1^2 , while b_1 occurs in no term of A_{22} ; whence, by (28₂), $A_{21} \equiv A_{22} \equiv 0$.

In $A_{32}a_1^3 b_2^2$, $e_1 = 3$, $f_2 = 2$, so that $e_3 = 1$. But $a_3 b_2^2$ can not be a factor since $A_{12} \equiv 0$. Hence $A_{32} \equiv 0$.

By (25₁), (23) and (28₁), $A_{31}a_3 = A_{31}a_2 = A_{31}b_1 = 0$. Hence A_{31} has the factor π (§ 11), contrary to (22). Hence $A_{31} \equiv 0$.

By (26₁), $A_{30}a_2 = 0$, so that $e_2 \equiv 0$ (mod 3). Hence $f_3 = 1$. But the factor $a_1^3 b_3$ can not occur since $A_{31} \equiv 0$. Hence $A_{30} \equiv 0$.

For A_{02} , $e_3 = 1$, whereas $a_3 b_2^2$ is not a factor. Hence $A_{02} \equiv 0$.

Since every $A_{i3} = A_{3i} = 0$, a factor a^3 or b^3 can not occur. Likewise, no factor $a_i b_j$, $a_i b_j^2$, $a_i^2 b_j$, $a_i^2 b_j^2$ ($i \neq j$) can occur. It thus follows readily from (33'') that

$$A_{10} = \alpha a_2 a_3, \quad A_{01} = \beta b_1 b_3 + \gamma a_2^2, \quad A_{20} = \delta b_1, \quad A_{00} = \varepsilon a_3^2 b_3,$$

the last following since $e_3 = 2$, so that b_1 can not occur.

From (31), $\beta = 0$, $\gamma = \alpha$, $\delta = \alpha$. Applying the permutation [23], we get $\varepsilon = \alpha$. Hence $\phi = S_3$.

14. On comparing the invariants of the ternary quadratic form (13) in the $GF[2^n]$ for the cases $n=1$ and $n=2$, we note uniformity in the invariants A, I, S_3 . In fact, these are invariants for any n . Corresponding to F in (50), there should be for $n=1$ an invariant analogous to f itself (compare § 6). We find that, for $n=1$, $I+J$ is precisely of the form f with the exponents omitted.

For $n=3$ the corresponding invariant must be of the form $f+f^2+f^4$. It would be natural to conjecture that f would be of the form (50) with exponents 3 changed to 7, and each a_i^1 changed to a_i^5 (in view of the weights). While the resulting terms do form a part of f , there occur 26 additional terms [see (91)].

15. We therefore proceed to investigate the invariants of the ternary form (13) in the $GF[2^3]$. Under transformation (14), let ϕ , with exponents ≤ 7 , become ϕ' . Using the same abbreviations as in § 11, we find that in $\phi' - \phi$ the coefficients of t, t^2, t^4 are, respectively:

$$\left. \begin{aligned} & a_2(1) + a_3(2) + b_1^4(2^4) + a_2^2 b_1^3(1^2 2^3) + a_2^4 b_1^2(1^4 2^2) + a_2^3 a_3 b_1^2(1^3 2^3) \\ & + a_2^4 b_1^2(2^6) + a_2^6 b_1(1^6 2) + a_2^4 a_3^2 b_1(1^4 2^3) + a_2^3 a_3^4 b_1(1^2 2^5) + a_3^6 b_1(2^7) \\ & + a_2^7 a_3(1^7 2) + a_2^6 a_3^2(1^6 2^2) + a_2^5 a_3^3(1^5 2^3) + a_2^4 a_3^4(1^4 2^4) + a_2^3 a_3^5(1^3 2^5) \\ & + a_2^2 a_3^6(1^2 2^6) + (a_2 a_3^7 + a_2 b_1^7)(1 2^7) + a_2^3 b_1^6(1^3 2^6) + a_2^2 a_3 b_1^6(1^2 2^7) \\ & + a_2^5 b_1^5(1^5 2^5) + a_2^3 a_3^2 b_1^5(1^3 2^7) + a_2^7 b_1^4(1^7 2^4) + a_2^6 a_3 b_1^4(1^6 2^5) \\ & + a_2^5 a_3^2 b_1^4(1^5 2^6) + a_2^4 a_3^3 b_1^4(1^4 2^7) + a_2^5 a_3^4 b_1^3(1^7 2^7) + a_2^7 a_3^4 b_1^2(1^7 2^6) \\ & + a_2^6 a_3^5 b_1^2(1^6 2^7) + a_2^7 a_3^6 b_1(1^7 2^7), \end{aligned} \right\} \quad (51)$$

$$\left. \begin{aligned} & b_1(2) + a_2^2(1^2) + a_2 a_3(1 2) + a_2^3(2^2) + a_2 b_1^4(1 2^4) + a_3 b_1^4(2^5) + a_2^3 b_1^3(1^3 2^3) \\ & + a_2^5 b_1^2(1^5 2^2) + a_2^4 a_3 b_1^2(1^4 2^3) + a_2 a_3^4 b_1^2(1 2^6) + a_3^5 b_1^2(2^7) + a_2^7 b_1(1^7 2) \\ & + a_2^5 a_3^2 b_1(1^5 2^3) + a_2^3 a_3^4 b_1(1^3 2^5) + a_2 a_3^6 b_1(1 2^7) + a_2^7 a_3^2(1^7 2^2) \\ & + a_2^6 a_3^3(1^6 2^3) + a_2^5 a_3^4(1^5 2^4) + a_2^4 a_3^5(1^4 2^5) + a_2^3 a_3^6(1^3 2^6) + a_2^2(a_3^7 + b_1^7)(1^2 2^7) \\ & + a_2^4 b_1^6(1^4 2^6) + a_2^3 a_3 b_1^6(1^3 2^7) + a_2^6 b_1^5(1^6 2^5) + a_2^4 a_3^2 b_1^5(1^4 2^7) + a_2^7 a_3 b_1^4(1^7 2^6) \\ & + a_2^6 a_3^2 b_1^4(1^6 2^6) + a_2^5 a_3^3 b_1^4(1^5 2^7) + a_2^6 a_3^4 b_1^3(1^6 2^7) + a_2^7 a_3^5 b_1^2(1^7 2^7), \end{aligned} \right\} \quad (52)$$

$$\left. \begin{aligned} & b_1^2(2^2) + a_2^2 b_1(1^2 2) + a_3^2 b_1(2^3) + a_2^4(1^4) + a_2^3 a_3(1^3 2) + a_2^2 a_3^2(1^2 2^2) \\ & + a_2 a_3^3(1 2^3) + a_3^4(2^4) + a_2 b_1^5(1 2^5) + a_2^3 b_1^4(1^3 2^4) + a_2^2 a_3 b_1^4(1^2 2^5) \\ & + a_2 a_3^2 b_1^4(1 2^6) + a_3^3 b_1^4(2^7) + a_2^5 b_1^3(1^5 2^3) + a_2 a_3^4 b_1^3(1 2^7) + a_2^7 b_1^2(1^7 2^2) \\ & + a_2^6 a_3 b_1^2(1^6 2^3) + a_2^3 a_3^4 b_1^2(1^3 2^6) + a_2^2 a_3^5 b_1^2(1^2 2^7) + a_2^7 a_3^2 b_1(1^7 2^3) \\ & + a_2^5 a_3^4 b_1(1^5 2^5) + a_2^3 a_3^6 b_1(1^3 2^7) + a_2^7 a_3^4 b_1(1^7 2^4) + a_2^6 a_3^5(1^6 2^5) + a_2^5 a_3^6(1^5 2^6) \\ & + a_2^4(a_3^7 + b_1^7)(1^4 2^7) + a_2^6 b_1^6(1^6 2^6) + a_2^5 a_3 b_1^6(1^5 2^7) + a_2^6 a_3^2 b_1^5(1^6 2^7) \\ & + a_2^7 a_3^3 b_1^4(1^7 2^7). \end{aligned} \right\} \quad (53)$$

We may set

$$\phi = \sum_{i,j}^{0,1,\dots,7} A_{ij} a_1^i b_2^j \quad (A_{ij} \text{ independent of } a_1, b_2). \quad (54)$$

We require that (51) shall vanish identically in a_1, b_2 for this value of ϕ . The simplest of the resulting conditions are:

$$A_{ij} a_2 = A_{ij} a_3 = A_{ij} b_1 = 0 \quad (i, j = 1, 7; 3, 7; 5, 7; 7, 7; 5, 5; 7, 5). \quad (55)$$

(The remaining conditions are considered later.) For these six A_{ij} ,

$$A_{ij} = \alpha_{ij} \pi, \quad \pi \equiv (a_2^7 - 1)(a_3^7 - 1)(b_1^7 - 1),$$

where α_{ij} is a function of b_3 only. Hence the factor of $a_1^7 b_2^7 a_3^7$ in ϕ is

$$\alpha_{77} (a_2^7 - 1)(b_1^7 - 1).$$

This must be symmetrical in b_1 and b_3 . Hence

$$\alpha_{77} = c (b_3^7 - 1), \quad c = \text{constant}.$$

On replacing ϕ by $\phi - c I$, where I is the absolute invariant given by (17) for $n=3$, we may set $A_{77} \equiv 0$. Hence no term of ϕ can have a factor $a_i^7 b_j^7 (i \neq j)$. Thus

$$A_{17} = A_{37} = A_{57} = A_{77} = A_{55} = A_{75} = 0. \quad (56)$$

Among the conditions that (52) shall vanish, when (56) holds, are (55) for $i, j = 2, 3; 2, 7; 3, 3; 6, 3; 6, 7; 7, 3$, and

$$A_{76} a_2 = A_{76} a_3 = A_{36} a_2 = A_{35} a_2 = 0.$$

Two of the conditions from (51) now reduce to $A_{76} b_1 = 0, A_{36} a_3 = 0$. Hence in A_{35} , there would be the factor $(a_3^7 - 1) b_2^5$, whereas $A_{75} \equiv 0$. Hence

$$A_{23} = A_{27} = A_{33} = A_{63} = A_{67} = A_{73} = A_{76} = A_{35} = 0, \quad A_{36} a_2 = 0. \quad (57)$$

When we apply (56) and (57) in computing (53), the conditions include :

$$\begin{aligned} A_{47} a_2 &= A_{47} a_3 = A_{47} b_1 = 0, & A_{65} a_2 &= A_{65} a_3 = 0, & A_{66} a_3 &= A_{66} b_1 = 0, \\ A_{56} a_3 &= A_{56} b_1 = 0, & A_{53} a_2 &= A_{53} b_1 = 0, & A_{46} a_3 &= A_{46} b_1 = 0. \end{aligned}$$

Hence

$$A_{47} = A_{66} = A_{56} = A_{53} = A_{46} = A_{65} = 0. \quad (58)$$

In view of (57) and (58), certain of the conditions from (51) give

$$A_{38} b_1 = 0, \quad A_{15} a_2 = A_{15} a_3 = A_{15} b_1 = 0.$$

But $A_{38} a_2 = 0$ by (57). Hence

$$A_{38} = 0, \quad A_{15} = 0. \quad (59)$$

The A_{ij} in (56), (57), (58) and (59) are the only ones which vanish in every invariant distinct from I , as may be seen by examining S_3^7 and (91). We have therefore reached the limit to the simplification due to the vanishing A_{ij} . We next give the conditions on the non-vanishing A_{ij} which result from (51)–(53). In a few instances a multiple of the left member of one condition has been subtracted from that of a longer condition.

$$A_{71}a_2 = A_{72}a_2 = A_{74}a_2 = 0, \quad (60)$$

$$A_{71}a_3 + A_{74}b_1^4 = 0, \quad A_{71}b_1 + A_{72}a_3^2 = 0, \quad A_{72}b_1^2 + A_{74}a_3^4 = 0, \quad (61)$$

$$A_{16}a_2 + A_{07}a_3 = 0, \quad A_{13}a_2 + A_{07}b_1^4 = 0, \quad A_{13}a_3 + A_{16}b_1^4 = 0, \quad (62)$$

$$A_{51}a_3 + A_{54}b_1^4 = 0, \quad A_{51}a_2 + A_{45}b_1^4 = 0, \quad A_{54}a_2 + A_{45}a_3 = 0, \quad (63)$$

$$A_{34}a_2 + A_{25}a_3 = 0, \quad A_{31}a_2 + A_{25}b_1^4 = 0, \quad A_{31}a_3 + A_{34}b_1^4 = 0, \quad (64)$$

$$A_{43}a_3 + A_{52}a_2 = 0, \quad A_{14}a_2 + A_{05}a_3 = 0, \quad A_{32}a_2 + A_{26}b_1^4 = 0, \quad (65)$$

$$A_{70}a_2 + A_{61}a_3 + A_{64}b_1^4 = 0, \quad A_{50}a_2 + A_{41}a_3 + A_{44}b_1^4 = 0, \quad (66)$$

$$A_{12}a_2 + A_{03}a_3 + A_{06}b_1^4 = 0, \quad A_{11}a_2 + A_{05}b_1^4 + A_{43}a_2^4b_1^2 = 0, \quad (67)$$

$$A_{11}a_3 + A_{14}b_1^4 + A_{52}a_2^4b_1^2 = 0, \quad A_{30}a_2 + A_{24}b_1^4 + A_{21}a_3 + A_{62}a_2^4b_1^2 = 0, \quad (68)$$

$$A_{10}a_2 + A_{01}a_3 + A_{04}b_1^4 + A_{42}a_2^4b_1^2 + A_{43}a_2^4a_3^2b_1 = 0, \quad (69)$$

$$A_{43}b_1 + A_{62}a_2^2 = 0, \quad A_{43}a_3^2 + A_{61}a_2^2 = 0, \quad A_{61}b_1 + A_{62}a_3^2 = 0, \quad (70)$$

$$A_{13}b_1 + A_{32}a_2^2 = 0, \quad A_{31}a_2^2 + A_{13}a_3^2 = 0, \quad A_{31}b_1 + A_{32}a_3^2 = 0, \quad (71)$$

$$A_{07}b_1 + A_{26}a_2^2 = 0, \quad A_{07}a_3^2 + A_{25}a_2^2 = 0, \quad A_{45}b_1 + A_{64}a_2^2 = 0, \quad (72)$$

$$A_{08}b_1 + A_{22}a_2^2 + A_{07}a_3b_1^4 = 0, \quad A_{05}b_1 + A_{24}a_2^2 + A_{06}a_3^2 = 0, \quad (73)$$

$$A_{03}a_3^2 + A_{21}a_2^2 = 0, \quad A_{70}a_2^2 + A_{51}b_1 + A_{52}a_3^2 = 0, \quad (74)$$

$$A_{21}b_1 + A_{22}a_3^2 + A_{25}a_3b_1^4 = 0, \quad A_{11}b_1 + A_{12}a_3^2 + A_{30}a_2^2 = 0, \quad (75)$$

$$A_{34}a_2^2 + A_{16}a_3^2 = 0, \quad A_{41}b_1 + A_{42}a_3^2 + A_{60}a_2^2 + A_{51}a_2a_3 = 0, \quad (76)$$

$$A_{01}b_1 + A_{02}a_3^2 + A_{20}a_2^2 + A_{14}a_2b_1^4 + A_{52}a_2^5b_1^2 = 0, \quad (77)$$

$$A_{07}b_1^2 + A_{45}a_2^4 = 0, \quad A_{07}a_3^4 + A_{43}a_2^4 = 0, \quad A_{45}a_3^4 + A_{43}b_1^2 = 0, \quad (78)$$

$$A_{16}b_1^2 + A_{54}a_2^4 = 0, \quad A_{16}a_3^4 + A_{52}a_2^4 = 0, \quad A_{54}a_3^4 + A_{52}b_1^2 = 0, \quad (79)$$

$$A_{26}b_1^2 + A_{64}a_2^4 = 0, \quad A_{26}a_3^4 + A_{62}a_2^4 = 0, \quad A_{64}a_3^4 + A_{62}b_1^2 = 0, \quad (80)$$

$$A_{06}a_3^4 + A_{42}a_2^4 = 0, \quad A_{51}a_2^4 + A_{13}b_1^2 = 0, \quad A_{25}a_3^4 + A_{61}a_2^4 = 0, \quad (81)$$

$$A_{06}b_1^2 + A_{25}a_2^2b_1 + A_{44}a_2^4 = 0, \quad A_{03}b_1^2 + A_{05}a_3^4 + A_{41}a_2^4 = 0, \quad (82)$$

$$A_{60}a_2^4 + A_{22}b_1^2 + A_{24}a_3^4 = 0, \quad A_{70}a_2^4 + A_{32}b_1^2 + A_{34}a_3^4 = 0, \quad (83)$$

$$A_{42}b_1^2 + A_{43}a_3^2b_1 + A_{44}a_3^4 = 0, \quad A_{12}b_1^2 + A_{50}a_2^4 + A_{32}a_2^2a_3^2 + A_{14}a_3^4 = 0, \quad (84)$$

$$A_{02}b_1^2 + A_{21}a_2^2b_1 + A_{03}a_3^2b_1 + A_{40}a_2^4 + A_{04}a_3^4 + A_{22}a_2^2a_3^2 = 0. \quad (85)$$

16. Let ϕ be an absolute invariant whose general term has the notation (32), with exponents satisfying

$$e_2 + e_3 + 2f_1 \equiv e_1 + e_3 + 2f_2 \equiv e_1 + e_2 + 2f_3 \equiv 0 \pmod{7}. \quad (86)$$

From (60) and (61) we get:

$$A_{71} = ra_3^5 b_1 (a_2^7 - 1), \quad A_{72} = ra_3^3 b_1^2 (a_2^7 - 1), \quad A_{74} = ra_3^6 b_1^4 (a_2^7 - 1).$$

Since the coefficient $\sum A_{7j} b_1^j$ of a_1^7 must be unaltered by [23],

$$A_{70} = r(a_2^3 b_1^2 b_3^2 + a_2^5 b_1 b_3 + a_2^6 b_1^4 b_3^4) (a_3^7 - 1) + ka_2^7 a_3^7 + la_2^7 + mb_1^7 + c.$$

From (86), (62), (63), (78₁), (71), (64), (72), (80), (70₃), (79₂), (78₃):

$$\begin{aligned} A_{07} &= \beta a_2^3 b_1^2 b_3^2 + \gamma a_2^5 b_1 b_3 + \delta a_2^6 b_1^4 b_3^4 + \varepsilon a_2^7, \\ A_{16} &= \beta a_2^2 a_3 b_1^2 b_3^2 + \gamma a_2^4 a_3 b_1 b_3 + \delta a_2^5 a_3 b_1^4 b_3^4 + \varepsilon a_2^6 a_3, \\ A_{18} &= \beta a_2^2 b_1^6 b_3^2 + \gamma a_2^4 b_1^5 b_3 + \delta a_2^5 b_1 b_3^4 + \varepsilon a_2^6 b_1^4, \\ A_{45} &= \beta a_2^6 b_1^4 b_3^2 + \gamma a_2 b_1^3 b_3 + \delta a_2^2 b_1^6 b_3^4 + \varepsilon a_2^3 b_1^2, \\ A_{54} &= \beta a_2^5 a_3 b_1^4 b_3^2 + \gamma a_2 a_3 b_1^3 b_3 + \delta a_2 a_3 b_1^6 b_3^4 + \varepsilon a_2^2 a_3 b_1^2, \\ A_{51} &= \beta a_2^5 b_1 b_3^2 + \gamma b_1^7 b_3 + \delta a_2 b_1^3 b_3^4 + \varepsilon a_2^2 b_1^6 + sb_3 (a_2^7 - 1) (a_3^7 - 1), \\ A_{31} &= \beta a_2^2 b_1^6 b_3^2 + \gamma a_2^2 a_3^2 b_1^5 b_3 + \delta a_2^3 a_3^2 b_1^4 b_3^4 + \varepsilon a_2^4 a_3^2 b_1^4, \\ A_{34} &= \beta a_2^3 b_1^2 b_3^2 + \gamma a_2^2 a_3^2 b_1 b_3 + \delta a_2^3 a_3^2 b_1^4 b_3^4 + \varepsilon a_2^4 a_3^2, \\ A_{25} &= \beta a_2 a_3^2 b_1^2 b_3^2 + \gamma a_2^3 a_3^2 b_1 b_3 + \delta a_2^4 a_3^2 b_1^4 b_3^4 + \varepsilon a_2^5 a_3^2, \\ A_{32} &= \beta b_1^7 b_3^2 + \gamma a_2^2 b_1^6 b_3 + \delta a_2^3 b_1^2 b_3^4 + \varepsilon a_2^4 b_1^5 + pb_3^2 (a_2^7 - 1) (a_3^7 - 1), \\ A_{26} &= \beta a_2 b_1^3 b_3^2 + \gamma a_2^3 b_1^2 b_3 + \delta a_2^4 b_1^5 b_3^4 + \varepsilon a_2^5 b_1, \\ A_{62} &= \beta a_2^4 a_3^4 b_1^3 b_3^2 + \gamma a_2^6 a_3^4 b_1^2 b_3 + \delta a_2^4 b_1^5 b_3^4 + \varepsilon a_2 a_3^4 b_1, \\ A_{64} &= \beta a_2^4 b_1^5 b_3^2 + \gamma a_2^6 b_1^4 b_3 + \delta b_1^7 b_3^4 + \varepsilon a_2 b_1^3 + qb_3^4 (a_2^7 - 1) (a_3^7 - 1), \\ A_{61} &= \beta a_2^4 a_3^6 b_1^2 b_3^2 + \gamma a_2^6 a_3^6 b_1 b_3 + \delta a_2^6 b_1^4 b_3^4 + \varepsilon a_2 a_3^6, \\ A_{52} &= \beta a_2^5 a_3^5 b_1^2 b_3^2 + \gamma a_2^5 b_1 b_3 + \delta a_2 a_3^5 b_1^4 b_3^4 + \varepsilon a_2^2 a_3^5, \\ A_{43} &= \beta a_2^6 a_3^4 b_1^2 b_3^2 + \gamma a_2 a_3^4 b_1 b_3 + \delta a_2^2 a_3^4 b_1^4 b_3^4 + \varepsilon a_2^3 a_3^4. \end{aligned}$$

In view of (66₁), (74₂) and (83₂),

$$\beta = \gamma = \delta = q = s = p = r, \quad m = \varepsilon, \quad c = l, \quad k = \varepsilon + l. \quad (87)$$

Since the coefficient $A_{05} + A_{25} a_1^2 + A_{45} a_1^4$ of b_2^5 in ϕ must be unaltered by the permutation [13], and likewise for the coefficient $A_{06} + A_{16} a_1 + A_{26} a_1^2$ of b_2^6 , and the coefficient $A_{03} + A_{13} a_1 + A_{43} a_1^4$ of b_2^3 , we get:

$$\begin{aligned} A_{05} &= ra_2 a_3^4 b_1 b_3^3 + ra_2^2 a_3^4 b_1^4 b_3^6 + ra_2^3 a_3^4 b_1^2 b_3^4 + \varepsilon a_2^3 a_3^4 b_3^2, \\ A_{06} &= ra_2^4 a_3^2 b_1^4 b_3^5 + ra_2 a_3^2 b_1^2 b_3^3 + ra_2^3 a_3^2 b_1^2 b_3^2 + \varepsilon a_2^5 a_3^2 b_3, \\ A_{03} &= ra_2^2 a_3 b_1^2 b_3^6 + ra_2^4 a_3 b_1 b_3^5 + ra_2^5 a_3 b_1^4 b_3 + \varepsilon a_2^6 a_3 b_3^4. \end{aligned}$$

By (65₂), (67₂), (68₁):

$$A_{14} = ra_3^5 b_1 b_3^3 + ra_2 a_3^5 b_1^4 b_3^6 + ra_2^5 a_3^5 b_1^2 b_3^4 + \varepsilon a_2^2 a_3^5 b_3^2,$$

$$A_{11} = ra_3^4 b_1^5 b_3^3 + ra_2 a_3^4 b_1^4 b_3^6 + ra_2^4 a_3^4 b_1^3 b_3 + (r + \varepsilon) a_2^2 a_3^4 b_1^4 b_3^2 + \varepsilon a_2^6 a_3^4 b_1^2.$$

By (67₁), (73), (74₁), (81₁), (82):

$$\begin{aligned} A_{12} &= ra_3^2 b_1^6 b_3^3 + ra_2 a_3^2 b_1^2 b_3^6 + ra_2^2 a_3^2 b_1^5 b_3^2 + (r + \epsilon) a_2^4 a_3^2 b_1^4 b_3 + \epsilon a_2^5 a_3^2 b_3^4, \\ A_{22} &= ra_3 b_1^3 b_3^6 + ra_2 a_3 b_1^6 b_3^2 + ra_2^2 a_3 b_1^2 b_3^5 + (r + \epsilon) a_2^4 a_3 b_1 b_3^4 + \epsilon a_2^5 a_3 b_1^4, \\ A_{24} &= ra_3^4 b_1^5 b_3^6 + ra_2^2 a_3^4 b_1^4 b_3^5 + ra_2^4 a_3^4 b_1^3 b_3^4 + (r + \epsilon) a_2 a_3^4 b_1 b_3^2 + \epsilon a_2^3 a_3^4 b_3, \\ A_{44} &= ra_3^2 b_1^6 b_3^5 + ra_2^2 a_3^2 b_1^5 b_3^4 + ra_2^4 a_3^2 b_1^4 b_3^3 + (r + \epsilon) a_2 a_3^2 b_1^2 b_3 + \epsilon a_2^3 a_3^2 b_1, \\ A_{41} &= ra_3 b_1^3 b_3^5 + ra_2 a_3 b_1^6 b_3 + ra_2^4 a_3 b_1 b_3^3 + (r + \epsilon) a_2^2 a_3 b_1^2 b_3^4 + \epsilon a_2^6 a_3 b_3^2, \\ A_{21} &= ra_3^3 b_1^2 b_3^6 + ra_2^2 a_3^3 b_1 b_3^5 + ra_2^3 a_3^3 b_1^4 b_3 + \epsilon a_2^4 a_3^3 b_3^4, \\ A_{42} &= ra_3^6 b_1^4 b_3^5 + ra_2^4 a_3^6 b_1^2 b_3^3 + ra_2^6 a_3^6 b_1 b_3^2 + \epsilon a_2 a_3^6 b_3. \end{aligned}$$

By (66₂), (75₂), (83₁):

$$\begin{aligned} A_{10} &= \epsilon a_3^2 (b_1^6 b_3 + a_2 b_1^2 b_3^4 + a_2^2 b_1^5 + a_2^5 b_3^2), \\ A_{30} &= \epsilon a_3^4 (b_1^5 b_3^2 + a_2^2 b_1^4 b_3 + a_2^4 b_1^3 + a_2^3 b_3^4), \\ A_{60} &= \epsilon a_3 (b_1^3 b_3^4 + a_2^4 b_1 b_3^2 + a_2 b_1^6 + a_2^6 b_3). \end{aligned}$$

It remains to determine A_{10} , A_{20} , A_{40} , A_{00} , A_{01} , A_{02} , A_{04} , which occur only in the three long conditions (69), (77) and (85). All the remaining conditions are seen to be now satisfied. Since the coefficient $\sum_{j=0}^7 A_{ij} b_2^j$ of a_1^i in ϕ must be unaltered by [23], we get for $i = 1, 2, 4$:

$$\begin{aligned} A_{10} &= \epsilon a_3^6 (b_1^4 b_3^3 + a_2 b_1^6 + a_2^4 b_1^2 b_3) + \lambda a_2^6 a_3^6 b_1, \\ A_{20} &= \epsilon a_3^5 (b_1 b_3^6 + a_2^2 b_1^5 + a_2 b_1^4 b_3^2) + \mu a_2^5 a_3^5 b_1^2, \\ A_{40} &= \epsilon a_3^3 (b_1^2 b_3^5 + a_2^4 b_1^3 + a_2^2 b_1 b_3^4) + \nu a_2^3 a_3^3 b_1^4. \end{aligned}$$

Since the terms $\sum A_{i0} a_1^i$ independent of b_2 are to be unaltered by [13],

$$\lambda = \mu = \nu = \epsilon, \quad (88)$$

while the terms of A_{00} which involve a_3 are:

$$la_3^7 + la_2^7 a_3^7 + \epsilon a_3^7 b_3^7 + ra_3^7 (a_2^5 b_1 b_3 + a_2^3 b_1^2 b_3^2 + a_2^6 b_1^4 b_3^4). \quad (89)$$

From the final conditions in (68), (77), (85), we now get:

$$\begin{aligned} A_{01} &= \rho a_3^5 b_1 + \sigma a_3^5 b_1 b_3^7 + ra_2 a_3^5 b_1^4 b_3^3 + \epsilon a_2^2 a_3^5 b_3^6 + ra_2^2 a_3^5 b_1^2 b_3 + \tau a_2^7 a_3^5 b_1, \\ A_{02} &= \rho a_3^3 b_1^2 + \sigma a_3^3 b_1^2 b_3^7 + ra_2^2 a_3^3 b_1 b_3^6 + \epsilon a_2^4 a_3^3 b_3^5 + ra_2^3 a_3^3 b_1^4 b_3^2 + \tau a_2^7 a_3^3 b_1^2, \\ A_{04} &= \rho a_3^6 b_1^4 + \sigma a_3^6 b_1^4 b_3^7 + ra_2^4 a_3^6 b_1^2 b_3^5 + \epsilon a_2 a_3^6 b_3^3 + ra_2^6 a_3^6 b_1 b_3^4 + \tau a_2^7 a_3^6 b_1^4. \end{aligned}$$

Since the term $\rho a_3^5 b_1 b_2$ of $A_{01} b_2$ corresponds to $\sigma a_1^5 b_2 b_3$ of $A_{51} a_1^5 b_2$, $\rho = \sigma = r$. Similarly, we can determine σ , τ and the parameters of A_{00} . We can do this at one step by requiring that the terms $A_{0j} b_2^j$, independent of a_1 , shall be unaltered by [23]. We find that

$$\rho = \sigma = \tau = r, \quad (90)$$

$$A_{00} = ra_2^3 b_1^2 b_3^6 + ra_2^5 b_1 b_3 + ra_2^6 b_1^4 b_3^4 + la_2^7 + l + \text{terms (89)},$$

where we have chosen the constant term of ϕ to be l .

In view of (87), (88) and (90), all the parameters occurring in the preceding expressions for the A_{ij} are expressed in terms of r, l, ε . That the remaining conditions (from the coefficients of $a_1^6, a_1^5, a_1^3, b_2^4, b_2^2, b_2$) for the invariance of ϕ under [13] and [23] are satisfied may be verified directly or from what follows. Hence ϕ is an absolute invariant with the three arbitrary parameters r, l, ε . Now l occurs only in A_{70} and A_{00} ; thus for $l = 1, r = \varepsilon = 0$, ϕ is the invariant A given by (17). For $\varepsilon = 1, r = l = 0$, ϕ is seen to equal S_3^7, S_3 given by (49). Finally, for $r = 1, l = \varepsilon = 0$, ϕ becomes

$$\left. \begin{aligned} F = f + f^2 + f^4, \quad f \equiv & \sum_3 a_1^5 b_2 b_3 (a_2^7 - 1) (a_3^7 - 1) + \sum_3 a_1^5 b_1^7 b_2 b_3 \\ & + \sum_3 a_1^5 a_2^5 b_1 b_2 b_3^2 + a_1^5 a_2^5 a_3^5 b_1^2 b_2^2 b_3^2 + \sum_3 a_1^5 a_2^5 a_3 b_1^4 b_2^4 b_3^2 \\ & + \sum_6 a_1^5 a_2 b_1^3 b_2 b_3^4 + \sum_3 a_1^5 a_2 a_3 b_1^6 b_2^4 b_3^4 + \sum_6 a_1 a_2^2 b_1^6 b_2^3 b_3^2 \\ & + \sum_3 a_1^2 a_2 a_3 b_1^6 b_2^2 b_3^2 + \sum_3 a_1^4 a_2 a_3 b_1^6 b_2 b_3 + a_1 a_2^2 a_3^4 b_1^4 b_2 b_3^2 + a_1 a_3^2 a_2^4 b_1^4 b_3 b_2^2. \end{aligned} \right\} \quad (91)$$

We note the relation $S_3 F = 0$.

17. From the conditions in § 15, we readily determine the relative invariants. As in § 13, it suffices to treat the case $d \equiv 2$. We first prove that $A_{07} = 0$, then that $A_{13} = A_{16} = 0$, etc., proceeding as in § 13. The result found is that *the only relative invariants are the powers of S_3* .

18. The results for the cases $n = 1, 2, 3$ differ only in the increasing complexity of the absolute invariant F . For $n = 4$, the investigation was limited to the determination of this invariant. The parameters λ were restricted to the values 0, 1, so that $\lambda^2 = \lambda$. Moreover, it was assumed that ϕ is identical with ϕ^2 in the $GF[2^4]$, so that the presence of any term implies the presence of its square, with the same coefficient (in view of $\lambda^2 = \lambda$). Thus from A_{ij} we deduce $A_{2i, 2j}$. The invariant thus determined is

$$F = f + f^2 + f^4 + f^8, \quad (92)$$

where

$$\begin{aligned} f = & \sum a_1^{13} b_2 b_3 (a_2^{15} - 1) (a_3^{15} - 1) + a_1^{13} a_2^{13} a_3^{13} b_1^2 b_2^2 b_3^2 + \sum a_1^{13} b_1^{15} b_2 b_3 + \sum a_1^{13} a_2^{13} b_1 b_2 b_3^2 \\ & + \sum a_1^{13} a_2^{13} a_3 b_1^8 b_2^8 b_3^2 + \sum a_1^{13} a_2 a_3 b_1^4 b_2^8 b_3^8 + \sum a_1^{13} a_2 b_1^7 b_2 b_3^8 + \sum a_1^{13} a_2^9 b_1^3 b_2 b_3^4 \\ & + \sum a_1^{13} a_2^{13} a_3^9 b_1^4 b_2^4 b_3^2 + \sum a_1^{13} a_2^9 a_3 b_1^{10} b_2^8 b_3^4 + \sum a_1^{13} a_2^9 a_3^9 b_1^6 b_2^4 b_3^4 + \sum a_1^{10} a_2 a_3 b_1^{14} b_2^2 b_3^2 \\ & + \sum a_1^{10} a_2 a_3 b_1^2 b_2^2 b_3^5 + \sum a_1^{12} a_2 a_3 b_1^{14} b_2 b_3 + \sum a_1^6 a_2 a_3 b_1^{14} b_2^4 b_3^4 + \sum a_1^{12} a_2^{12} a_3 b_1 b_2 b_3^3 \\ & + \sum a_1^6 a_2 a_3 b_1^4 b_2^4 b_3^9 + \sum a_1^6 a_3 b_1^7 b_2^4 b_3^{12} + \sum a_1^{12} a_3 b_1^7 b_2 b_3^9 + \sum a_1^6 a_2^5 a_3 b_1^{12} b_2^4 b_3^2 \\ & + \sum a_1^6 a_2^4 a_3 b_1^5 b_2^4 b_3^{10} + \sum a_1^6 a_2^8 a_3 b_1^3 b_2^4 b_3^8 + \sum a_1^{12} a_2^{10} a_3 b_1^2 b_2 b_3^4 + \sum a_1^{12} a_2^8 a_3 b_1^3 b_2 b_3^5 \\ & + \sum a_1^{10} a_2^8 a_3 b_1^3 b_2^2 b_3^6 + \sum a_1^6 a_2^6 a_3^5 b_1^2 b_2^2 b_3^9 + \sum a_1^6 a_2^5 a_3^5 b_1^{10} b_2^2 b_3^2 + \sum a_1^6 a_2^5 b_1^5 b_2^{12} b_3^2 \\ & + \sum a_1^8 a_2^5 a_3 b_1^{12} b_2^2 b_3 + \sum a_1^8 a_2^4 a_3 b_1^5 b_2^3 b_3^9 + \sum a_1^5 a_2^9 a_3 b_1^{10} b_2^2 b_3^8 + \sum a_1^{10} a_2 a_3 b_1^7 b_2^{10} b_3^2. \end{aligned}$$

19. The invariants obtained for $n \leq 4$ were expressed in terms of A, I, S_3 and F (F denoting $I + J$ when $n = 1$). In each case we have noted the relation $S_3 F = 0$. Since every term of S_3 and F involves one or more a 's, $AS_3 = AF = 0$. By inspection,

$$A^2 = A, \quad I^2 = I, \quad F^2 = F, \quad AI = I, \quad IS_3 = IF = 0, \quad S_3^{2^n} = S_3.$$

By means of these relations we may express the product of any two invariants as a linear function of A, I, F, S_3^i ($i = 1, \dots, 2^n - 1$). The latter may be taken as the units of a linear associative algebra with coördinates in the $GF[2^n]$.

20. *As a set of independent invariants we may take*

$$A, \quad S_3, \quad J \quad (J = F + I).$$

Indeed, $AJ = I$. Next, to show that, for example, S_3 is independent of A and J , it suffices to exhibit two sets of values of the coefficients a_i, b_i , for which A has the same value, J the same value, but S_3 different values. Such a proof of the independence of A, S_3, J follows by inspection from the table below. From §§ 2, 6, we obtain a complete set of canonical forms of ternary quadratic forms in the $GF[2^n]$. In the second form, ρ is a particular solution of $\chi(\rho) = 1$; for $n = 1$ or 3, we may take $\rho = 1$. We note that $F = \chi(f)$, where

$$f = \sum a_1^{\mu-2} b_2 b_3 (a_2^{\mu} - 1) (a_3^{\mu} - 1) + \text{terms with factor } b_1 b_2 b_3,$$

μ denoting $2^n - 1$. Thus $F = \chi(\rho^2) = 1$ for the second form, $F = 0$ for the others.

Canonical form	S_3	A	J
$x_1 x_2 + x_3^2$	1	0	0
$x_1 x_2 + \rho x_1^2 + \rho x_2^2$	0	0	1
$x_1 x_2$	0	0	0
x_1^2	0	1	0
Vanishing form	0	1	1

The five types are characterized by the respective sets of values:

$$S_3 = 1; \quad A = 0, J = 1; \quad S_3 = A = J = 0; \quad A = 1, J = 0; \quad A = J = 1.$$

THE UNIVERSITY OF CHICAGO, October, 1906.